FSA Integration Partner Program

United States Department of Education

Office of Federal Student Aid

Final Security and Privacy Architecture Report

Deliverable 124.1.2

Task Order 124:

Security and Privacy Architecture Framework

Version 1.0

DRAFT

May 30, 2003

Confidential – For Official Use Only

Document Revision History

Version Number	Date	Author	Revisions Made
1.0	May 30, 2003	Hector G. Mezquida, Jesse Bowen	Initial draft published

Table of Contents

1 Executive Summary

This document is a required deliverable for Federal Student Aid Task Order 124 – Security and Privacy Architecture Framework. It consists of two major sections:

- Section 3 – Final Status Report provides an overview of activities and results from this task order.
- Section 4 -- Implementation Strategy for the FSA Security and Privacy Architecture defines major recommendations for implementing architecture services and components.

The proposed FSA Security and Privacy Architecture vision consists of security services, technical components, and standards to guide planning and development of security. Each component is defined in detail, along with implementation considerations, in deliverable 124.1.3 – Security and Privacy Architecture Specification

This report makes six major recommendations for implementing the FSA security architecture:

- Develop and execute a communications plan to socialize existing FSA policy and procedures.
- Perform a gap analysis and develop standards and procedures needed to implement the security and privacy architecture vision.
- Assess the effectiveness of the System Security Officer Program for communicating and enforcing FSA security and privacy architecture standards
- Deploy an Identity Management Service
- Deploy an Access Management Service
- Create security and privacy architecture standards that can be incorporated into contracts and agreements with third parties for outsourced services.

High-level implementation steps, planning considerations, and a proposed schedule are described in Section 4 to deploy an Identity Management Service and an Access Management Service.

2 Introduction

2.1 Objectives

This is the Final Report for Task Order 124 – Security and Privacy Architecture Framework. This document contains a summary of work accomplished during this effort, and presents recommendations for planning and implementation of a Security and Privacy Architecture Framework for the Office of Federal Student Aid (FSA). The recommendations include a discussion of development and deployment strategies for components of the Security and Privacy Architecture envisioned for FSA. Next steps are suggested for the period immediately following the conclusion of this task order.

2.2 Scope

This report covers work defined in Task Order 124 related to definition of technical components for a security and privacy architecture framework. The intent of this effort was to define technical security solutions and services. Security policy and process components of an overall security architecture was not within the scope of this work. However, as depicted in Figure 2.1, an effective security capability includes more than just technology components. This diagram (from deliverable 124.1.1 Interim Security and Privacy Architecture Report) shows the major security domains in the model, consisting of security management and security processes in addition to technical security controls. Security policy and process elements will be critical to successful deployment of security and privacy technologies. Policy and process considerations are included in some of the recommendations where they constitute prerequisite or integral elements of technical security components.

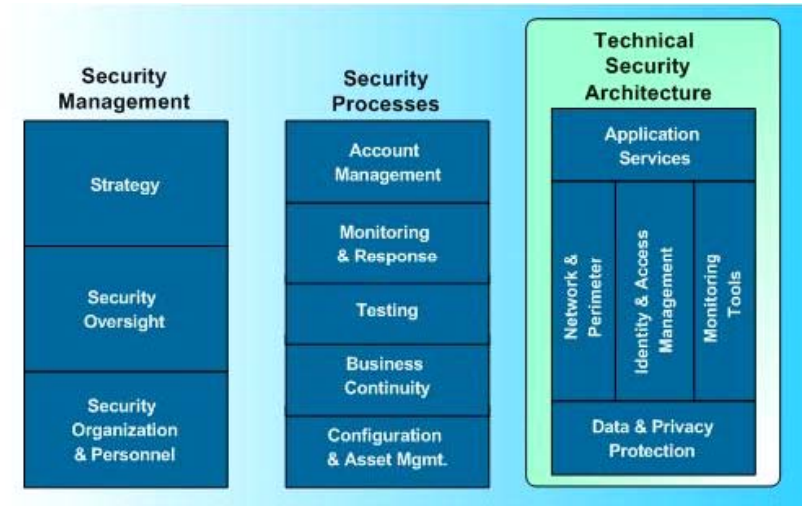

Figure 2.1. Generic Security and Privacy Framework, as defined in deliverable 124.1.1 Interim Security and Privacy Architecture Framework[1]

[1] The referenced deliverable contains an explanation of the generic framework structure, including detailed functional and technical descriptions of the 22 major components that comprise the five control areas in the Technical Security Architecture layer.

This implementation strategy applies to the initial version (Version 1.0) of the FSA Security Architecture, as proposed in deliverable 124.1.3 Security and Privacy Architecture Framework Specification. Once adopted, the FSA Security and Privacy Architecture vision will need periodic review and updating. The architecture description should remain a dynamic conceptual framework that incorporates changes in FSA plans, requirements, and deployment efforts. This implies that the implementation recommendations, considerations, and strategies discussed in this report should not be considered final. Additional FSA security objectives and specific requirements will be defined by system and application development efforts, as well as related projects that are part of the Data Strategy task order. The implementation strategy defined in this document, as well as the Security and Privacy Architecture Specification itself, must be reviewed and modified as appropriate to satisfy requirements that result.

2.3 Organization of This Document

This deliverable provides a final status report on work conducted as part of Task Order 124. This report also describes recommendations and an implementation strategy for deploying the FSA Security and Privacy Architecture Framework.

This document consists of three major sections, described briefly below:

- Section 3 – *Final Task Order Status Report* provides an overview of the project objectives, discusses the activities conducted as part of the task order, and summarizes the task order results and deliverables.
- Section 4 – *Implementation Strategy for the FSA Security and Privacy Architecture* reviews principles and assumptions that guided development of an implementation strategy, summarizes the implementation recommendations, presents a planning overview for deployment of security and privacy architecture components, and discusses scheduling considerations.
- Section 5 – *Conclusions and Next Steps* describes recommended next steps to continue development of the FSA security and privacy architecture vision, and to prepare for deployment of recommended technology components.

This document is meant as a companion deliverable to 124.1.3 Security and Privacy Architecture Specification. The architecture specification defines business objectives for security that were identified during this task order. It also presents and explains a proposed security and privacy architecture specification to satisfy the FSA security objectives.

3 Final Task Order Status Report

3.1 Project Overview

The goal of the Security and Privacy Architecture Framework task order was to define an overall vision to guide planning and development of FSA security and privacy technical services and components. The ultimate objective of the security and privacy architecture framework is to increase FSA's effectiveness in the following critical protection areas:

- Integrity – Prevent data theft from FSA and maximize transactional accuracy.
- Confidentiality – Prevent unauthorized viewing or alteration of other people's data.
- Availability – Prevent service disruption.
- Accountability – Provide for clean security audits.

The specific purpose of this task order was to produce the first version of a Security and Privacy Architecture Framework, in cooperation with FSA business units, contractors, and partners. To accomplish this, the following tasks were planned:

- Conduct a Security Architecture Workshop.
- Develop a Generic Framework for the FSA Security and Privacy Architecture.
- Develop an FSA Security and Privacy Architecture Framework Specification.
- Define a Security and Privacy Architecture Implementation Strategy.

3.2 Activities

TO124 – Security and Privacy Architecture Framework – commenced on February 28, 2003. The task order was designed to run for approximately three months, concluding May 30, 2003. Three major deliverables were planned, as described in section 3.3 below.

An initial project kickoff meeting and security workshop was scheduled and held on March 6, 2003. The participants and minutes from the workshop meeting are summarized in Section 4 of deliverable 124.1.1 Interim Security and Privacy Architecture Report. Information-gathering meeting were also held with business and technology subject matter experts, System Security Officers, and the FSA Business Integration Group. An iterative approach was used to identify and validate security and privacy business objectives. A proposed Security and Privacy Architecture Specification was then created that can meet the business security objectives defined during the course of this task order.

Previous work to address security and privacy controls were reviewed as input to development of the vision for FSA security and privacy technology architecture. The relevant FSA documentation included:

- FSA Information Technology Security and Privacy Policy (March 2003 draft)
- FSA Security Solution Lifecycle Guide (December 17, 2002)
- Deliverables from Task Order 82 – Single Sign-On Requirements and Design, 2002

- 16.1.2 – Integrated Integrated Technical Architecture Detailed Design Document, Volume 5 – Security Architecture (deliverable from Task Order 16 – Integrated Technical Architecture Design), 2000
- The E-Authentication Gateway – Connecting People to Services, GSA White Paper, June 13, 2002
- e-Authentication Initiative Program Overview, GSA eGov Implementation Guide, 2002

Project teams from ongoing task orders were consulted to gather and validate business security objectives. These teams were briefed on the goals and progress of the Security and Privacy Architecture task order, and input was solicited to understand the relationship with their work. Representatives from the following teams were included in this effort:

- Consistent Data
- Technical Strategies
- XML Framework
- Common Student ID
- Routing ID
- Enrollment and Access Management
- Enterprise Application Integration
- Integrated Technical Architecture
- Case Management Office
- Students Portal

3.3 Results and Deliverables Overview

Draft deliverables as specified in the task order (and described in Section 3.3, below) were completed by the required due dates. The original goal for this effort was to then move directly into a pilot implementation phase to deploy one or more security services for FSA. Due to changes in emphasis, FSA decided to delay the pilot implementation phase until after additional requirements related to security and privacy are collected and analyzed by other task orders, primarily the Data Strategy effort. This Final Report includes discussion of implementation strategies for the Security and Privacy Architecture. But interim activities are also included that can benefit FSA security goals before deployment of security technology solutions begins during the next fiscal year.

The deliverables created by this task order are summarized below.

3.3.1 Interim Security and Privacy Architecture Report

Deliverable Designation: 124.1.1

Date Draft Delivered: April 4, 2003

Date Final Version Delivered: April 25, 2003

Summary of Contents: Task Order Interim Status Report
Security Workshop Meeting Minutes
Preliminary Security Business Objectives
Generic Security Framework

3.3.2 Final Security and Privacy Architecture Report

Deliverable Designation:	124.1.2
Date Draft Delivered:	May 30, 2003
Date Final Version Delivered:	June 20, 2003 (Planned)
Summary of Contents:	Final Task Order Status Report Implementation Strategy for Security and Privacy Architecture Conclusions and Next Steps

3.3.3 Security and Privacy Architecture Framework Specification

Deliverable Designation:	124.1.3
Date Draft Delivered:	May 30, 2003
Date Final Version Delivered:	June 20, 2003 (Planned)
Summary of Contents:	Security and Privacy Architecture Objectives Security Process Model for Identity and Access Management Security and Privacy Business Requirements Proposed Security and Privacy Architecture Specification Validation of Security and Privacy Architecture

4 Implementation Strategy for the FSA Security and Privacy Architecture

4.1 Background

The proposed FSA Security and Privacy Architecture vision consists of security services, technical components, and standards to guide planning and development of security (see Figure 4.1). This section describes a strategy for implementing security architecture services and components. The strategy accounts for the differing natures of the proposed security architecture components. Some of the components are proposed for deployment as services available across multiple systems. For these elements of the infrastructure, the implementation strategy will describe planning, design, and development considerations. Some components (mostly related to network and infrastructure functions) will be primarily the responsibility of vendors or third parties who provide outsourced services. Other components will require development of standards primarily for the consumption of FSA development teams. Architecture components that involve creation of standards will be addressed by defining the types of standards and describing examples of requirements that should be included in them.

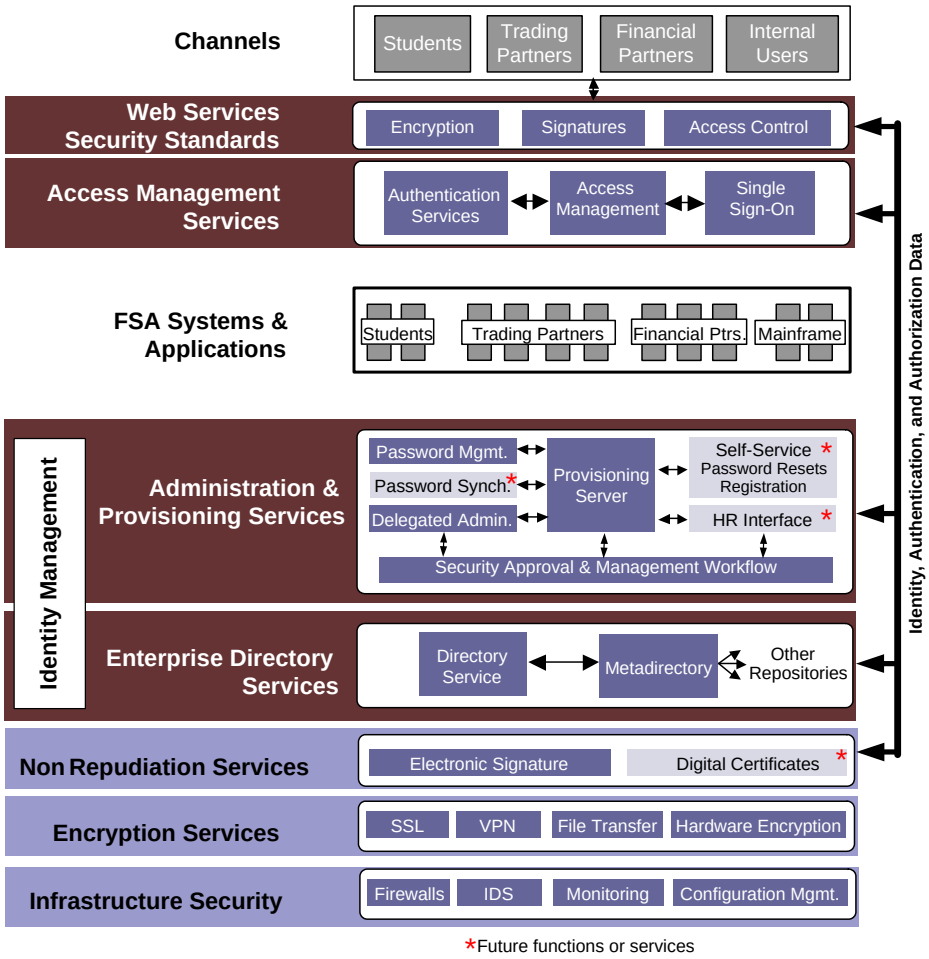

Figure 4.1. Proposed FSA Security and Privacy Architecture framework (see 124.1.3 – Security and Privacy Architecture Specification for details)

4.1.1 Use of the FSA Security and Privacy Architecture

The final FSA Security and Privacy Architecture specification will provide an important tool for the design and deployment of security measures. The architecture can be used:

- As a guide for security strategy and planning
- As a security design and deployment aid to promote structured, systematic, and repeatable development of security controls
- To communicate technical standards and decisions, both internally and externally
- As part of the FSA Solution Life Cycle to:
    - Integrate security architecture checkpoints into SLC checklists (e.g., during the vision, definition, and construction phases)
    - Describe how designers and developers can take advantage of existing security solutions or services to avoid custom builds
    - Align technical system design and configuration with FSA security policy
- To capture successful and proven security solutions for future use
- To document security architecture updates based on analysis of results from development projects and changes in system or technology requirements.

The security architecture is not a design or a detailed implementation plan. It is intended as reference vision for the major security services and components needed to satisfy FSA security requirements. The architecture description provides high-level direction and standards for selecting technology solutions. Deployment of the technical security services described later in this section must be accompanied by additional detailed design steps to create the actual implementation plan. However, this strategy describes the major steps required for developing the plan, and discusses overall timing and other planning considerations.

4.1.2 Architecture Deployment Principles

Development of an implementation approach for the FSA Security and Privacy Architecture was driven by several principles and considerations about the unique aspects of the FSA computing environment. These principles and assumptions are summarized below.

- *FSA wishes to create and promote an architectural framework for security and privacy services and standards.*
  In the past, decisions about system-specific protections were decentralized. Business units allocated business funds to pay for system controls or to share in the cost of infrastructure upgrades. To decrease deployment and maintenance costs, and to avoid duplicate investments, the FSA security and privacy architecture should define security services and standards that apply across system and business unit boundaries
- *The FSA computing environment is heavily outsourced.*
  Most system design, development, testing, and operations work is contracted out to vendors and other third parties. FSA security architecture components must support outsourced operations through standards and requirements that become incorporated into contractual outsourcing agreements.

- *The Federal Student Aid program has a unique security environment.*
  FSA relies on continual data exchange with schools, state agencies, and private lenders. FSA systems are used by a variety of groups, including students, their parents, school financial aid administrators, and financial partners. This means the FSA security architecture implementation strategy must incorporate a high degree of flexibility for implementing security controls that fit the different risk profiles and access privileges of these diverse groups.

- *The Security and Privacy Architecture implementation strategy must effectively support FSA business objectives.*
  Business objectives that affect security should be continually validated against the security and privacy architecture vision. Business units should be involved throughout the planning and deployment stages for security services and components. Security requirements should be coordinated across projects that are defining functional requirements for FSA data and systems.

- *Security and privacy architecture components should be deployed in modular units.*
  Deployment of security components and services should be planned in manageable increments that represent feasible deployment efforts while still providing demonstrable benefits. Security functions should be designed and deployed to enhance flexibility and reuse, both for systems and applications and for other components of the architecture. As an example, authentication services can be defined or deployed that remain discrete from other access management functions, to allow configuration of authentication levels suitable for specific user groups. Similarly, a directory service could be deployed as a discrete function to make it available for both access management and identity management systems.

- *Isolated, "one-off" security solutions should be minimized.*
  To be effective, the security and privacy architecture implementation strategy must begin integration with existing development projects. Since security services will require time to complete analysis, design, and build activities, situations will probably arise where, because of timing or specific requirements, a special-purpose or interim solution can be justified. However, a process should also be developed to obtain approval for the exception, and to create a plan for future integration of the exception solution into the FSA Security and Privacy Architecture.

- *Deployment of standard security services does not preclude multiple instances of approved solutions.*
  Although the security architecture vision depicts single components for each type of functionality, this does not necessarily imply that only a single instance of each capability will be required. For example, the Access Management Service could be multiple instances. However, a standard set of products and components should be used to prevent proliferation of divergent but similar solutions. This approach to use of security architecture standards will decrease licensing costs, complexity, training requirements, and maintenance overhead.

4.2 Implementation Recommendations

This section summarizes major recommendations for implementation of an FSA security and privacy architecture. These recommendations are based on FSA business objectives related to security, in the context of the overall FSA technical architecture and sourcing strategy.

4.2.1 Implementation Overview

FSA serves a diverse user population through an extensive, heterogeneous set of systems and applications. No single set of technology solutions are likely to satisfy all FSA business objectives. This implies that security functional requirements may also vary between systems. However, many commonalities exist among FSA systems, and a security and privacy architecture can be developed to serve as a unifying and consistent vision of technology approaches to deploying reusable services and components. The recommendations below deal with three major elements of the deployment effort:

1. Define, communicate, and enforce a security and privacy policy framework to support the security architecture;
2. Deploy a set of technology components to provide consistent security functionality
3. Create consistent standards and requirements for technical and security functions that are outsourced to contractors and vendors.

Recommendations in each of these three areas are outlined below.

4.2.2 Policy Prerequisites for the FSA Security and Privacy Architecture

A sound policy framework is a necessary prerequisite for effective deployment of an FSA security and privacy architecture. Several elements of the FSA policy framework are either already in place or currently in development:

- The draft FSA Information Technology Security and Privacy Policy is a good foundation for the more detailed standards, processes, and procedures that must be in place to support and enforce security architecture components.
- Ongoing efforts to complete the FSA Certification and Accreditation process will help individual systems document their current security posture and plan security controls. When completed, the ongoing Certification and Accreditation process will help monitor system compliance with FSA policies.
- The FSA Security Solution Lifecycle Guide and implementation plan will promote integration of security and privacy reviews and standards into the system development process.

In addition to these efforts, policies, standards, and organizational structures will need to be modified to enable effective deployment of an FSA security and privacy architecture. The following three recommendations address the major efforts that should be considered prerequisites for creating and implementing security architecture technology components.

Recommendation 1: Develop and execute a communications plan to socialize existing FSA policy and procedures.

From conversations with system and business representatives, it is apparent that the current FSA IT Security and Privacy Policy is not fully understood or used across FSA systems. The Certification and Accreditation process currently underway will provide a mechanism to convey FSA security requirements to system managers and technical leads. However, additional steps should be taken to promote feedback and acceptance of the draft policy. The communications plan should address the following areas:

- Provide an overview of the scope, roles and responsibilities, and security controls defined in the policy
- Help system owners and responsible parties understand how the policy applies to their specific systems
- Solicit feedback from system owners as a means of enhancing understanding and acceptance of the policy
- Provide a process for identifying security areas or issues that may need additional augmentation or interpretation for specific situations
- Describe the process FSA will use to monitor and track compliance with the security policy
- Define the process for periodic review and updating of the FSA policy to maintain currency with changes in threats, technologies, and requirements.

Recommendation 2: Perform a gap analysis and develop standards and procedures needed to implement the security and privacy architecture vision.

Deployment of the FSA Security and Privacy Architecture will require development of technology standards. These standards will provide more detailed guidance than is available in the FSA IT Security and Privacy Policy, and may also require modification or development of new policies and procedures. An assessment of the standards required should be conducted to identify the existing policies and procedures that may need to be addressed. The following list describes examples of standards that should be considered.

Examples of relevant standards are described in the following sections.

Data classification standards

There is no formal set of data classification standards now, but these should be developed in conjunction with the Data Strategy task order. Possible classifications, suggested by the Security Workshop held as part of requirements gathering, are:

- Personal/private (Privacy Act information; personal or sensitive information)
- Financial data (concerning individuals)
- Financial integrity data (financial transactions, payments, etc.)
- Operational data (less sensitive; operations data for FSA, schools, financial partners)
- Public (unrestricted, non-sensitive data)

Data classifications can be used to define authorization standards and access privileges for specific groups of users.

Enterprise authorization standards and access roles

Currently, each FSA system defines its own standards and access control rules to decide which users need access to FSA systems and information assets. Standards defined across FSA will help improve the consistency of how access privileges are granted, based on job functions and the 'Need-to-Know' and 'Need-to-Do' principle defined in the FSA IT Security and Privacy policy. Enterprise standards can also be developed to create user roles that define access privileges across multiple FSA systems.

System-specific interpretations of general policy guidelines

The FSA IT Security and Privacy Policy defines FSA security controls at a high level (see Appendix 9.2 in 124.1.3 – Security and Privacy Architecture Specification for a summary). Additional standards and procedures will need to be developed to respond to specific needs. An example of a such a specific security issue, raised during a meeting with the Business Integration Group, is the concept of 'transient trust'. This principle allows an organization to accept the authentication credentials (perhaps including attributes that define access privileges) that were issued and validated by an external organization on behalf of a third party. Current policy defines a need for authentication and access control, but does not address this specific topic.

Standards for web services security

Web services are an importance component of FSA technical and data strategies. FSA will need standards to define security requirements for securing communication channels, verifying the identity of entities requesting or processing web services requests, and communicating user security privileges. Web services security standards should be developed to address the following areas:

- Securing existing web services transmissions with current technologies such as SSL
- The process to follow for identifying additional security requirements and needs as new web service functionality is added
- Procedures for following the development of new security standards and incorporating them into FSA architecture standards
- Evaluating and implementing security toolkits and SDKs available to implement web services security standards (e.g., WS-Security, SAML, XML-sig, XML-enc)
- Defining and documenting security integration points with business partners.

Electronic signature standards

Current FSA practice for electronic signatures is to rely on user authentication and an audit trail to validate online signing transactions. Although more robust procedures have been discussed (such as the use of digital signatures for non-repudiation of signatures and validation of transactions) there is not yet a compelling business case for their use. Even so, enterprise standards for acceptable procedures and controls to govern online signing should be developed. Standards and procedures for issues such as required level of authentication, audit trail requirements, and record retention procedures are typically developed on a case-by-case basis. This creates the potential for inconsistent application of security policies and controls.

Security and Privacy Architecture Implementation and Monitoring Standards

Standards should be developed to govern the maintenance and application of the Security and Privacy Architecture itself. Review steps that check conformance with the security architecture vision and requirements could be incorporated into the FSA Security Solution Lifecycle. Procedures should be included for obtaining approval of exceptions to the security architecture vision, and require planning for future integrated with the architecture standards to limit proliferation of non-standard solutions.

Recommendation 3: Assess the effectiveness of the System Security Officer Program for communicating and enforcing FSA security and privacy architecture standards

The System Security Officer (SSO) program has the potential to be a powerful mechanism for promoting and enforcing security architecture standards. However, work conducted during the course of this task order indicated that training and oversight of SSOs may need improvement. There is a large variation in the security background of SSOs, and hence their effectiveness in making and enforcing security decisions. This situation may limit the ability of the current SSO program as a mechanism for communicating and enforcing FSA security architecture standards, for several reasons:

- Lack of SSO familiarity with basic security principles and threat and risk assessment methodologies
- Little experience with evaluating and selecting security controls to address risks
- The decentralized nature of SSO governance.

The SSO Program should be assessed and recommendations developed to address gaps that may be identified. The assessment should cover the SSO selection process; governance and monitoring of SSO activities; and training or education requirements.

4.2.3 Technology Services and Components

There are two major security services that should be the focus of initial development for the FSA Security and Privacy Architecture. These services will provide identity management functions, such as centralized administration and user provisioning, and access management functions, such as authentication services, access control, and simplified sign-on.

Recommendation 4: Deploy an Identity Management Service

An identity management service provides a several important administrative functions and benefits, as described in Table 4.1 below. At a minimum, an identity management system will require components for centralized user access account administration, resource provisioning, and an identity data repository. Additional functions are typically available to provide functions such as password management, password synchronization, delegated administration, and self-service functionality. These additional functions can be added as needed after the basic identity management system is deployed.

A high-level implementation strategy for an identity management system is described in Section 4.3. The strategy includes major steps in the implementation, planning considerations, and examples of vendor products that provide related security functions.

Table 4.1. Major Functions and Benefits of an Identity Management Service

Functions	Benefits
• Centralize security administration • Provide tools for delegating selected administrative tasks to external organizations • Automate provisioning of user access accounts • Manage password policies • User self-service password reset or registration • Workflow for security approval and setup • Consolidate identity data stores • Maintain consistent identity data repositories • Synchronize identity data across heterogeneous environments	• Reduce application maintenance costs • Decrease time lag for obtaining access • Better control of terminated accounts • Facilitate regulatory compliance and audits • Reduce help desk calls with self-service • Improved accuracy of identity data • Improved consistency of identity data across enterprise

Recommendation 5: Deploy an Access Management Service

An access management service will provide authentication and access control functions for new or existing systems and applications. Through application interfaces and external calls, systems can obtain the benefits of robust, flexible security functions without creating duplicative functions within each application. Table 4.2 summarizes the functions and benefits of an Access Management Service.

Table 4.2. Major Functions and Benefits of an Access Management Service

Functions	Benefits
• Consolidate authentication services • Consolidate access control services • Accommodate flexible authentication requirements for differing user populations • Simplify sign-on across multiple systems • Reduce number of user IDs and passwords • Provide policy-based authorization rules	• Improved consistency of authentication • Improved consistency of access privileges across systems • Improved speed of system delivery • Decreased cost of system development

Access Management systems provide the ability to consolidate user login steps for multiple applications. This allows a user to sign-on once and obtain access to a group of systems or applications that have been configured to use the single sign-on service. Since it is rare to consolidate all systems that a user needs access to, ‘simplified sign-on’ is a more accurate description of this function than ‘single sign-on’.

An Access Management Service is most practical for web applications and portals. Vendor products are available to extend some access management functions to mainframe and legacy systems, but the effort required to effectively deploy such a capability usually outweighs the benefits. A more effective approach, and the general strategy being pursued by FSA, is to provide a web front-end user interface to legacy and mainframe applications.

Section 4.3 provides an overview of implementation steps and planning considerations for deployment of Access Management Services.

4.2.4 External Standards and Requirements for Outsourced Functions

For security functions that FSA outsources to contractors or vendors, it is impractical to deploy architecture services or detailed specifications. For example, an outsourced data center would typically be expected to provide access control and filtering functions for network traffic. It would not be feasible to specify products or comprehensive configuration standards. However, to support the goals of the FSA Security and Privacy Architecture, standards and requirements that conform to FSA business objectives.

Recommendation 6: Create security and privacy architecture standards that can be incorporated into contracts and agreements with third parties for outsourced services.

FSA security standards should be enforced through specific requirements and Service Level Agreements for security functionality. Examples of functions and services that should be included in contract bidding and negotiation include:

- Firewall administration procedures and response times
- Intrusion detection capabilities and reporting of security incidents
- Security testing, both at time of deployment and periodically, of networks, servers, and systems or applications
- Security configuration management issues, e.g., response times and procedures for analyzing, testing, and applying security patches and upgrades to network and operating system software.

4.3 Implementation Planning

4.3.1 Overview

This section describes implementation planning considerations for technical components of the proposed FSA Security and Privacy Architecture. Planning considerations are presented for two major security services: Identity Management Services and Access Management Services.

For each security service, the following deployment considerations will be described:

- High-level implementation steps and sequencing
- Dependencies
- Example commercial vendors

4.3.2 Identity Management Service Deployment

An Identity Management Service will require, at a minimum, an administration and resource provisioning system and a directory server or other identity data repository. Depending on specific requirements, a metadirectory system may also be required to connect disparate identity databases; alternatively, some metadirectory systems provide identity management functions. Additional functions that can be optionally deployed as part of an Identity Management System include security approval workflow tools and password synchronization systems. The central administration and resource provisioning system should be the primary focus of initial implementation efforts. Additional functionality can then be added as requirements warrant.

High-Level Implementation Steps and Sequencing

Figure 4.2 shows major phases and steps in the pilot and implementation of Identity Management components. Implementation should be conducted in phases that pilot the process and technology components, then integrate additional applications in manageable groups.

Pilot and Initial Release

The pilot phase will provide an opportunity to prototype the Identity Management system and develop processes for subsequent releases. A set of applications or systems will need to be selected for both the pilot and initial release stages. These would typically be the same or a similar set of applications. The piloting phases include steps for definition of selection criteria. A formal evaluation and selection process for pilot systems should be developed to set expectations of the candidate pilot areas and insure commitment to the goals and schedule of the pilot project. Following successful completion of the pilot, an initial release should be planned. The initial release should include integration with a small number of systems or applications; integration of between two and four systems or applications will demonstrate the benefits of identity management yet still represents a manageable effort for implementation.

Second and Subsequent Releases

Additional applications can be staged for later releases of the Identity Management system. Experience at deploying components in the FSA environment can be incorporated in follow-on releases to decrease the time required for analysis, design, and build activities. The analysis and design phases of subsequent releases can overlap with

the build activities of the initial release. However, the pilot deployment should be completed before beginning the design phase for later releases.

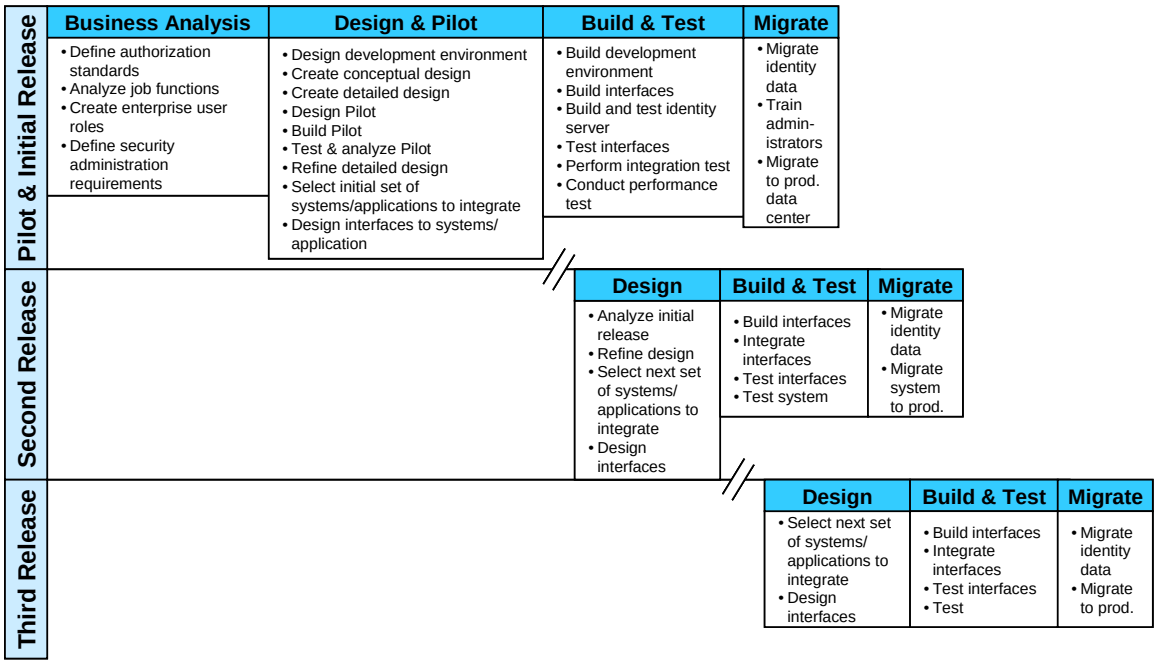

Figure 4.2. Overview of Identity Management Implementation Steps

Major Dependencies

- General: Business analysis must be performed to understand FSA authorization and user role requirements among the different user populations for FSA systems and applications.
- Centralized administration and resource provisioning
    - Systems and applications must be selected for pilot and initial releases
    - Account administration requirements must be defined for each system to be integrated
    - Policies and standards must be defined to guide system configuration of functions such as password management settings, account management processes, disabling inactive accounts, and removing terminated users
- Delegated administration
    - The centralized administration and resource provisioning server must be deployed
    - FSA must create policy and standards to define processes for approving and configuring responsibilities for delegation of security administration functions
- Enterprise Directory Service
    - Define system-of-record
    - Define the data migration strategy

Example Commercial Vendors for Identity Management Products

User Administration and Resource Provisioning Systems

- BMC Software – Control-SA
- Business Layers – eProvision
- IBM – Identity Manager
- Thor Technologies – Xelerate
- Waveset – Lighthouse

Enterprise Directories and Metadirectories

- Critical Path – CP Directory, CP Metadirectory
- Microsoft – Active Directory, Identity Manager
- Netegrity – IdentityMinder
- Novell – eDirectory, DirXML
- Oracle – Oracle Internet Directory
- Siemens -- DirXmetahub
- Sun – Sun ONE Directory Server, Sun ONE Metadirectory

4.3.3 Access Management Service Deployment

An Access Management Service consists of an access control system, an authentication service, and associated repositories for user data and access control policies or rules. Single sign-on or simplified sign-on functions can be included, but sets of related applications should be carefully selected based on commonality of function or user populations.

High-Level Implementation Steps and Sequencing

Figure 4.3 shows major phases in the implementation of an Access Management System. An important step in deployment planning will be selection of the systems or applications to be integrated into the Access Management System, and the design of the integration strategy. Applications and web portals can be configured to use an Access Management Service in a variety of ways: as an authentication service only; as an authentication and access control service; or in a hybrid fashion that divides access control functionality between the application and the Access Management System.

Pilot and Initial Release

The pilot effort will provide an opportunity to explore the most effective integration approaches for FSA systems and applications. Web applications or portals should be selected for the pilot and initial release that have a moderate number of users to minimize the impact of piloting and testing the new functionality. If possible, the pilot and initial release should be coordinated with a new release of the target system to avoid retrofitting application interfaces and security functions to existing designs.

Subsequent Releases

Later releases of the Access Management System can extend its functionality to additional systems or applications. The Access Management System can also be integrated with the Identity Management System to enable provisioning of users and applications in the web environment.

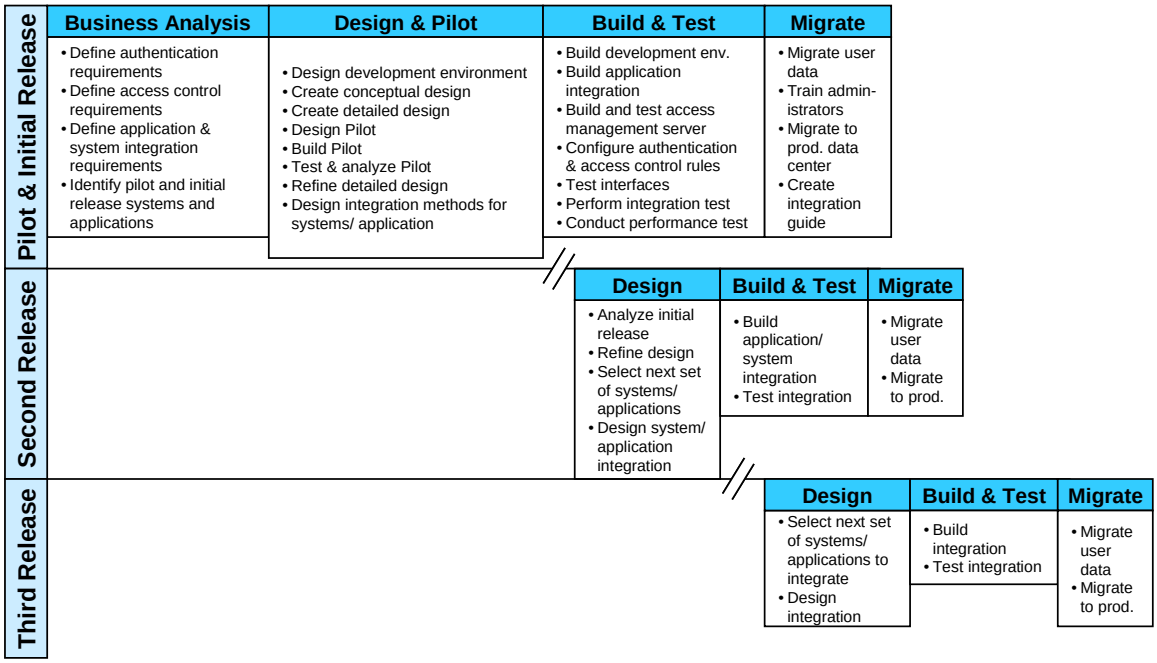

Figure 4.3. Overview of Access Management Implementation Steps

Major Dependencies

- Access management system
  - Access requirements and user roles must be defined for applications that will be integrated with the Access Management System
  - A Directory Service or other repository must be available to store user security data and access control policies or rules
  - Systems or applications must be selected for integration with the pilot, initial release, and subsequent releases
  - An application integration strategy must be created for systems or application to be integrated with the Access Management System
  - Authentication levels must be defined for each user group and resource that will be managed
  - If required, custom development may be needed to obtain data from external sources for dynamic access control rules.
- Simplified sign-on function
  - The Access Management System must be deployed

- Systems or applications must be selected to integrate as a set with the simplified sign-on function.

Example Commercial Vendors for Access Management Systems

- Entrust – getAccess
- IBM – Access Manager
- Netegrity – Siteminder, TransactionMinder
- Oblix – NetPoint
- RSA – Cleartrust

4.4 Overall Implementation Schedule and Roadmap

The comments below describe an overall approach to implementation of the various Security and Privacy Architecture components. While this section presents possible approaches to scheduling and sequencing component delivery, additional information will be needed to make final plans for the most effective implementation approach. Inputs to the final plan should include requirements from related projects (Data Strategy, PIN Site Reengineering Analysis, eAuthentication Gateway) and the FSA budgeting process. Information expected from these projects is discussed in more detail in section 4.4.2 below.

4.4.1 Timing Considerations for Services and Component Implementation

An example schedule for deployment of Security and Privacy Architecture components is shown in Figure 4.4. An Identity Management solution is shown as the first technology component to begin piloting. While early in development there are few absolute dependencies between access management and identity management technologies, FSA is currently engaged in a Data Strategy effort that is, among other thins, defining access requirements for several FSA user populations. Thus, the Access Management deployment is shown beginning near the end of that effort, in approximately four months. The advantage of delaying the Access Management implementation is that work on the Identity Management system will include development of a directory service that can in leveraged for both systems.

Implementation of Identity Management technologies typically does not require changes in existing systems or applications. This makes technical integration of identity management more straightforward for systems or applications that are already in product, since there is minimum impact on the existing capabilities. In contrast, integration of applications with an access management system usually requires more effort. For example, communication of user and credential information must be established, and session management must be coordinated with existing applications or portals.

Standards development is depicted in the schedule in two major categories:

- Internal standards to guide creation of the architecture and adherence to it by new development
- External standards for outsourcing arrangements

Internal standards for data classification, authorization, and user roles are prerequisites for deployment of an identity management solution, so they are shown as beginning first. Web services security standards and electronic signature standards are also important for FSA web services strategy, so they should also begin over the next several months.

External standards for communication to contractors and vendors can begin immediately. However, deployment of these standards will need to be coordinated with negotiations that take place during initiation or renewal of contractual arrangements.

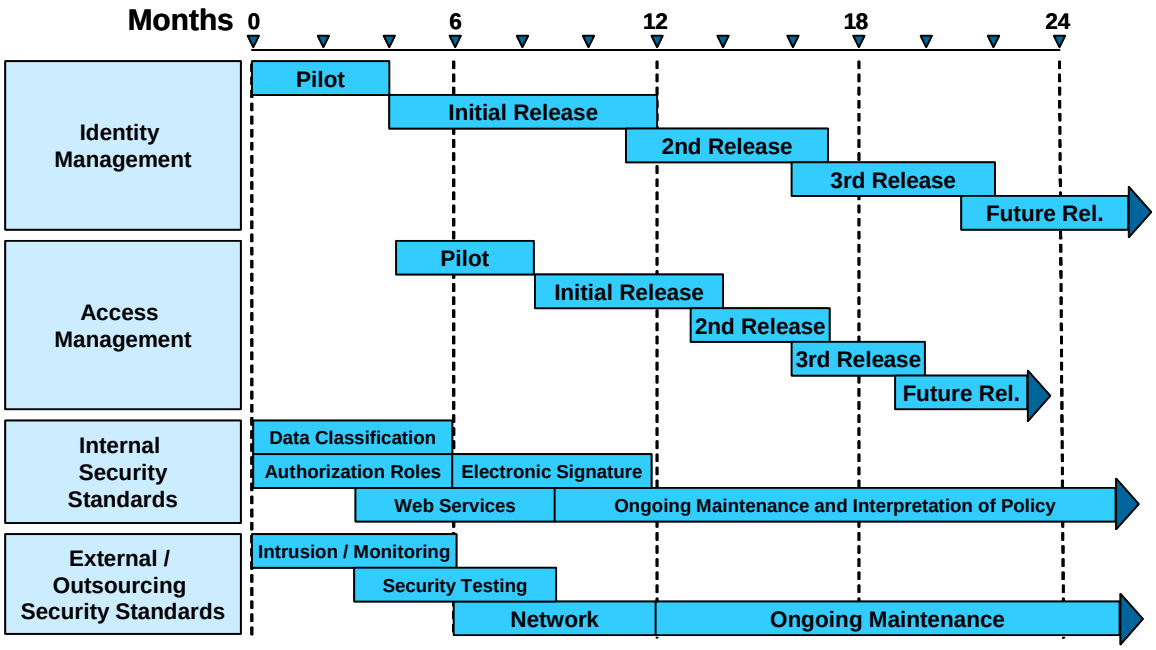

Figure 4.4. Sample Schedule for Implementation of Security and Privacy Architecture Components

4.4.2 Dependencies

Deployment of Security and Privacy Architecture components will require input from several other ongoing FSA efforts. Relevant projects and the types of input to be expected from them are defined in the list below. Note, however, that the security architecture effort need not wait to begin until all these projects are completed. There will be value in beginning communication of the overall vision defined in the architecture to guide the collection and analysis of requirements that result from the Data Strategy efforts.

- Data Strategy
  - Consistent Data — Data framework, data classification requirements
  - XML Framework — Web Services Security requirements
  - Common Student ID — Identifier requirements
  - Routing ID — Identifier and organization requirements
  - Enrollment and Access Management — Organization and user registration requirements
- Integrated Technical Architecture — Data center environment requirements
- Case Management Office — Access requirements, auditing requirements
- Students Portal — Portal security requirements (authentication, access control, auditing)
- PIN Site Reengineering Analysis — Authentication requirements, auditing requirements, electronic signature requirements

Conclusions and Next Steps

The Security and Privacy Architecture Framework task order has started the process of developing an FSA Security and Privacy Architecture by proposing an overall vision of the major components, services, and standards it should include. Several additional steps must be taken to continue making progress toward that goal.

- Continue validating the proposed vision for security architecture services and components as additional requirements are identified
- Prepare and plan for deployment of security architecture components: technology by planning product evaluations and pilot projects to validate the recommended approach
- Define the budgeting requirements to develop the initial set of security architecture services and components
- Communicate the FSA Security and Privacy Architecture vision throughout the FSA CIO organization and FSA business units.
- Integrate the FSA Security and Privacy Architecture vision into the overall FSA technical architecture
- Begin promoting adoption of the Security and Privacy Architecture vision by including review steps in the FSA Security Software Lifecycle